

WE CLAIM:

1. A method for generating identification data, comprising the steps of:
 providing a first set of identification data related to a first transaction type; and
 performing a cryptographic operation upon the first set of identification data, thereby
 generating a second set of identification data related to a second transaction type.

2. A method according to claim 1, wherein the step of performing a cryptographic operation comprises:
 providing a conversion key; and
 using the conversion key to perform said cryptographic operation upon the first set of identification data.

3. A method according to claim 2, wherein the step of providing a conversion key comprises:
 providing conversion key derivation data;
 providing a conversion key derivation key; and
 performing a cryptographic operation upon the conversion key derivation data and the conversion key derivation key.

1 4. A method according to claim 3, wherein the step of performing a cryptographic
2 operation upon the conversion key derivation data and the conversion key derivation key
3 comprises using the conversion key derivation key to perform at least one cryptographic
4 operation upon the conversion key derivation data.

1 5. A method according to claim 4, wherein the conversion key derivation data
2 includes an identification number that is associated with multiple accounts, and wherein at least
3 one cryptographic operation using a secret key is performed to cryptographically process said
4 conversion key derivation data to produce the conversion key.

1 6. A method according to claim 1, wherein the step of performing a cryptographic
2 operation comprises:
3 providing cryptographically-computed data; and
4 performing an operation upon the first set of identification data and the cryptographically-
5 computed data.

1 7. A method according to claim 6, wherein the step of providing cryptographically-
2 computed data comprises:
3 providing initial data; and
4 performing at least one cryptographic operation using a secret key upon the initial data,

5 thereby producing the cryptographically-computed data.

1 8. A method according to claim 7, wherein said at least one cryptographic operation
2 using a secret key comprises at least one of a DES-encryption and a DES-decryption.

1 9. A method according to claim 8, wherein at least a portion of the initial data is
2 obtained from at least a portion of an account number.

10. A method according to claim 9, wherein the operation upon the first set of
2 identification data and the cryptographically-computed data comprises either a subtraction
3 operation or an addition operation.

1 11. A method according to claim 10, wherein the step of providing cryptographically-
2 computed data further comprises generating a cryptographically-computed number having a base
3 corresponding to a base of a number representing the first set of identification data, wherein said
4 cryptographically-computed number has a number of digits corresponding to a number of digits
5 of said number representing the first set of identification data.

1 12. A method according to claim 6, wherein the step of providing cryptographically-
2 computed data comprises generating a cryptographically-computed number having a base

3 corresponding to a base of a number representing the first set of identification data, wherein said
 4 cryptographically-computed number has a number of digits corresponding to a number of digits
 5 of said number representing the first set of identification data.

1 13. A method according to claim 6, wherein the operation upon the first set of
 2 identification data and the cryptographically-computed data comprises either a subtraction
 3 operation or an addition operation.

14. A method for generating a cryptography key, comprising:
 providing a key derivation key;
 using the key derivation key in a cryptographic operation performed on data obtained
 from an identification number, thereby producing the cryptographic key.

15. A method according to claim 14, further comprising generating a key-check value
 suitable for determining whether data received corresponds to the cryptography key.

16. A method according to claim 15, wherein the step of generating a key-check value
 comprises:
 using a portion of the cryptography key to DES-encrypt a system-wide constant, thereby
 producing a first key-check value generation result;

5 using a portion of the cryptography key to DES-decrypt the first key-check value
 6 generation result, thereby producing a second key-check value generation result;
 7 using a portion of the cryptography key to DES-encrypt the second key-check value
 8 generation result, thereby producing a third key-check value generation result; and
 9 selecting a portion of the third key-check value generation result for use as a key-check
 10 value.

17. A system for generating identification data, comprising:

2 a memory for storing a first set of identification data related to a first transaction type;
 3 and
 4 a processor for performing a cryptographic operation upon the first set of data, such that
 5 said processor generates a second set of identification data related to a second transaction type.

18. The system of claim 17, wherein the memory includes means for storing a
 2 conversion key, and wherein the processor comprises means for using the conversion key to
 3 perform a cryptographic operation upon the first set of identification data.

19. The system of claim 18, wherein the memory further includes:

2 means for storing conversion key derivation data; and

3 means for storing a conversion key derivation key; and

4 wherein the processor comprises means to perform a cryptographic operation upon the
5 conversion key derivation data and the conversion key derivation key, thereby generating the
6 conversion key.

1 20. The system of claim 19, wherein the cryptographic operation upon the conversion
2 key derivation data and the conversion key derivation key comprises at least one DES operation.

3 21. The system of claim 20, wherein the conversion key derivation data is derived
4 from an identification number, and wherein said at least one DES operation comprises:

5 using a portion of the conversion key derivation key to DES-encrypt the conversion key
6 derivation data, thereby producing a first conversion key generation result;

7 using a portion of the conversion key derivation key to DES-decrypt the first conversion
8 key generation result, thereby producing a second conversion key generation result;

9 using a portion of the conversion key derivation key to DES-encrypt the second
10 conversion key generation result, thereby producing a third conversion key generation result;

11 using the third conversion key generation result as a first portion of the conversion key;

12 using a portion of the conversion key derivation key to DES-encrypt the third conversion
13 key generation result, thereby producing a fourth conversion key generation result;

using a portion of the conversion key derivation key to DES-decrypt the fourth

conversion key generation result, thereby producing a fifth conversion key generation result;

14 using a portion of the conversion key derivation key to DES-encrypt the fifth conversion
15 key generation result, thereby producing a sixth conversion key generation result; and
16 using the sixth conversion key generation result as a second portion of the conversion
17 key.

22. The system of claim 17, wherein the memory includes means for storing cryptographically-computed data, and wherein the processor comprises:

- means for generating the cryptographically-computed data; and
- means for performing an operation upon the first set of identification data and the cryptographically-computed data.

23. The system of claim 22, wherein the memory further includes means for storing initial data, and wherein the means for generating the cryptographically-computed data comprises means for performing at least one cryptographic operation upon the initial data, thereby producing the cryptographically-computed data.

24. The system of claim 23, wherein said at least one cryptographic operation comprises at least one of a DES-encryption and a DES-decryption.

25. The system of claim 24, wherein the initial data is obtained from an account

number, wherein the memory further includes means for storing a conversion key, and wherein the cryptographic operation uses the initial data and the conversion key to produce the cryptographically-computed data.

26. The system of claim 25, wherein the means for performing an operation upon the first set of identification data and the cryptographically-computed data comprises either a subtraction means or an addition means.

27. The system of claim 25, wherein the means for performing an operation further comprises means for generating a cryptographically-computed number having a base corresponding to a base of a number representing the first set of identification data, wherein said cryptographically-computed number has a number of digits corresponding to a number of digits of said number representing the first set of identification data.

28. The system of claim 22, wherein the means for performing an operation comprises means for generating a cryptographically-computed number having a base corresponding to a base of a number representing the first set of identification data, wherein said cryptographically-computed number has a number of digits corresponding to a number of digits of said number representing the first set of identification data.

1 29. The system of claim 22, wherein the means for performing an operation
2 comprises either a subtraction means or an addition means.

1 30. A system for generating a cryptography key, comprising:
2 a memory, comprising
3 means for storing a key derivation key; and
4 means for using the key derivation key in a cryptographic operation performed on
5 data obtained from an identification number, thereby producing the cryptographic key.

1 31. The system of claim 30, further comprising means for receiving data, wherein the
2 processor further comprises means for generating a key-check value suitable for determining
3 whether the data corresponds to the cryptography key.

1 32. The system of claim 31, wherein the means for generating a key-check value
2 comprises:
3 means for storing a system-wide constant;
4 means for using a portion of the cryptography key to DES-encrypt the system-wide
5 constant, thereby producing a first key-check value generation result;
6 means for using a portion of the cryptography key to DES-decrypt the first key-check
7 value generation result, thereby producing a second key-check value generation result;

8 means for using a portion of the cryptography key to DES-encrypt the second key-check
 9 value generation result, thereby producing a third key-check value generation result; and
 10 means for selecting a portion of the third key-check value generation result for use as a
 11 key-check value.

1 33. A system for generating identification data, comprising:
 2 a memory;
 3 a processor in communication with the memory; and
 4 a computer-readable medium in communication with the processor and storing
 5 instructions which, when executed, cause the processor to perform the steps of:
 6 storing a first set of identification data in the memory, said first set being related
 7 to a first transaction type; and
 8 performing a cryptographic operation upon the first set of identification data,
 9 thereby generating a second set of identification data related to a second transaction type.

1 34. The system of claim 33, wherein the step of performing a cryptographic operation
 2 comprises:
 3 providing a conversion key;
 4 storing the conversion key in the memory; and
 5 using the conversion key to perform said cryptographic operation upon the first set of

6 identification data.

1 35. The system of claim 34, wherein the step of providing a conversion key
comprises:

3 storing conversion key derivation data in the memory;

4 storing a conversion key derivation key in the memory; and

5 performing a cryptographic operation upon the conversion key derivation data and the
6 conversion key derivation key.

1 36. The system of claim 35, wherein the step of performing a cryptographic operation
2 upon the conversion key derivation data and the conversion key derivation key comprises using
3 the conversion key derivation key to perform at least one DES operation upon the conversion key
4 derivation data.

1 37. The system of claim 36, wherein the conversion key derivation data is derived
2 from an identification number, and wherein said at least one DES operation comprises:
3 using a portion of the conversion key derivation key to DES-encrypt the conversion key
4 derivation data, thereby producing a first conversion key generation result;
5 using a portion of the conversion key derivation key to DES-decrypt the first conversion
6 key generation result, thereby producing a second conversion key generation result;

7 using a portion of the conversion key derivation key to DES-encrypt the second
 8 conversion key generation result, thereby producing a third conversion key generation result;
 9 using the third conversion key generation result as a first portion of the conversion key;
 10 using a portion of the conversion key derivation key to DES-encrypt the third conversion
 11 *C* key generation result, thereby producing a fourth conversion key generation result;
 12 using a portion of the conversion key derivation key to DES-decrypt the fourth
 13 conversion key generation result, thereby producing a fifth conversion key generation result;
 14 using a portion of the conversion key derivation key to DES-encrypt the fifth conversion
 15 key generation result, thereby producing a sixth conversion key generation result; and
 16 using the sixth conversion key generation result as a second portion of the conversion
 17 key.
 18
 19
 20
 21
 22
 23
 24
 25
 26
 27
 28
 29
 30
 31
 32
 33
 34
 35
 36
 37

1 *sub a* 38. The system of claim 33, wherein the step of performing a cryptographic operation
 2 comprises:

3 providing cryptographically-computed data;
 4 storing the cryptographically-computed data in the memory; and
 5 performing an operation upon the first set of identification data and the cryptographically-
 6 computed data.

1 39. The system of claim 38, wherein the step of providing cryptographically-
 2 computed data comprises:

3 storing initial data in the memory; and
 4 performing at least one cryptographic operation using a secret key upon the initial data,
 5 thereby producing the cryptographically-computed data.

1 40. The system of claim 39, wherein said at least one cryptographic operation using a
 2 secret key comprises at least one of a DES-encryption and a DES-decryption.

1 41. A method according to claim 40, wherein at least a portion of the initial data is
 2 obtained from at least a portion of an account number.

1 42. The system of claim 41, wherein the operation upon the first set of identification
 2 data and the cryptographically-computed data comprises either a subtraction operation or an
 3 addition operation.

1 43. The system of claim 42, wherein the step of providing cryptographically-
 2 computed data further comprises generating a cryptographically-computed number having a base
 3 corresponding to a base of a number representing the first set of identification data, wherein said
 4 cryptographically-computed number has a number of digits corresponding to a number of digits

of said number representing the first set of identification data.

44. The system of claim 38, wherein the step of providing cryptographically-computed data comprises generating a cryptographically-computed number having a base corresponding to a base of a number representing the first set of identification data, wherein said cryptographically-computed number has a number of digits corresponding to a number of digits of said number representing the first set of identification data.

45. The system of claim 38, wherein the operation upon the first set of identification data and the cryptographically-computed data comprises either a subtraction operation or an addition operation.

46. A system for generating a cryptography key, comprising:
 a memory;
 a processor in communication with the memory; and
 a computer-readable medium in communication with the processor and storing instructions which, when executed, cause the processor to perform the steps of:
 storing a key derivation key in the memory;
 using the key derivation key in a cryptographic operation performed on data obtained from an identification number, thereby producing the cryptographic key.

Sub C1

47. The system of claim 46, wherein the instructions, when executed, further cause the processor to perform the step of generating a key-check value suitable for determining whether data received corresponds to the cryptography key.

48. The system of claim 47, wherein the step of generating a key-check value comprises:

- storing a system-wide constant in the memory;
- using a portion of the cryptography key to DES-encrypt the system-wide constant, thereby producing a first key-check value generation result;
- using a portion of the cryptography key to DES-decrypt the first key-check value generation result, thereby producing a second key-check value generation result;
- using a portion of the cryptography key to DES-encrypt the second key-check value generation result, thereby producing a third key-check value generation result; and
- selecting a portion of the third key-check value generation result for use as a key-check value.

Sub 5

49. A method for generating identification data for an electronic financial transaction over a communications network, comprising the steps of:

- providing a first set of identification data related to a first transaction type;

performing a cryptographic operation upon the first set of identification data to generate a second set of identification data for use in conducting said electronic financial transaction.

The method of claim 49, wherein said first set of identification data is an ATM-PIN, said first transaction type is an ATM-transaction, said second set of identification data is an electronic commerce PIN, said electronic financial transaction is an electronic commerce transaction, said method further comprising the step of:
performing a second cryptographic operation upon said electronic commerce PIN to generate said ATM-PIN.